Submission to the

Intelligence and Security Committee

Privacy and Security Inquiry

Prof Thomas W Simpson
Associate Professor of Philosophy and Public Policy
Blavatnik School of Government
University of Oxford

Professor John Naughton
Senior Research Fellow
Centre for Research in the Arts, Social Sciences and Humanities
University of Cambridge

BSG
OXFORD

CRASSH

Executive Summary

We welcome the ISC's inquiry into the laws which govern the intelligence agencies' interception of private communications. The Snowden revelations have made imperative a national discussion of the balance between individual liberties and the powers of the state in pursuing collective security, in particular regarding the bulk collection of metadata. In this submission, we identify the fundamental moral and political issues at stake. We argue that the balance is overly skewed in favour of security and give four recommendations for policy change in response. This is in answer principally to the questions raised under (a) in the Call for Evidence.

The UK Government should cease the bulk collection of metadata. In non-totalitarian states, there is an established moral norm that citizens' lives should be free from Government surveillance and investigation, unless there is reasonable suspicion of criminality. The burden of proof is on those who would revise this norm to show that it is necessary for an acceptable level of security. Two arguments are commonly given to show that, since the arrival of the Internet, things have changed sufficiently significantly that that norm should be revised—based on changing notions of privacy and increased threats. We show both of these arguments to be fallacious. The consequence of ceasing the bulk collection of metadata is that the UK will forego the opportunity to develop a new kind of capability in the service of security, namely that based on predictive analytics. This is a loss, but it is a sacrifice worth making to preserve the character of an open, democratic society. The UK will not forego the opportunity to investigate individuals who are the subject of reasonable suspicion of criminality or terrorism. For the metadata will still be available, albeit accessible only from the private corporations to whom the data was originally disclosed with the consent of the individuals to whom the data refer.

We give two further policy recommendations. The degree of disclosure of private information yielded by metadata is equivalent to that gained by tailing someone. So access to it should be classified in the same way as directed surveillance. This would constitute a raise in the evidential bar required for access by Government agencies. Additionally, the Interception of Communications Commissioner should be supported by advisor(s) with the appropriate technical expertise, in addition to the Commissioner's legal expertise.

This submission represents our personal views and not those of our respective institutions.

Authors. **Prof Tom Simpson** is Associate Professor of Philosophy and Public Policy at the Blavatnik School of Government, University of Oxford. He works on the ethics of security and technology, and previously served as an officer with the Royal Marines Commandos. Contact: thomas.simpson@bsg.ox.ac.uk. **Prof John Naughton** is Senior Research Fellow at the Centre for Arts, Social Sciences and Humanities (CRASSH), University of Cambridge. He is also Emeritus Professor for the Public Understanding of Technology at the Open University; Vice-President of Wolfson College, Cambridge; and the Technology columnist for the *Observer*. Contact: naughton@pobox.com.

Fundamental principles

1. We assume widespread agreement regarding the validity of the fundamental principles at stake. The 'first duty' of the sovereign is to protect society from the violence of others, as Adam Smith famously stated (*Wealth of Nations*, V.I.I). Nonetheless, the state exists for the sake of its individual members. That duty is therefore constrained by my interest in preserving my freedom, as well as other values I or we cherish. Thomas Hobbes gave the rule of thumb for the individual. I should 'be contented with so much liberty against other men as [I] would allow other men' against myself (*Leviathan*, §14). The heuristic is a useful guide for the kinds of coercive force the state should be willing to exercise: it should act coercively only in the ways required to preserve liberty.

2. One freedom we expect to be preserved is privacy. The boundary between public and private is culturally determined. Given that the boundary exists and that it exists *here*, we reasonably expect others not to breach it, including the state. The exception to this is in situations of severe, imminent threat to the survival of society, or where it is required for the prevention or punishment of criminality.

3. Privacy is valuable for both individual and societal reasons. As well as obvious personal reasons to want privacy, some societal values cannot be realised without it. A lively democracy requires freedom of association. We reasonably expect others not to know whom we have met with, and not to make efforts to find out in the absence of due suspicion of criminality or betrayal. For I am subject to an unspoken restricting influence if I must worry about others knowing who I spend time with. Reading is another practice subject to the same unspoken restricting influence, if I must worry about others' knowledge of my choices. So the privacy required for anonymous reading is justified on the same basis.

4. There is no single distinction between public and private. Rather, different domains of life—often differentiated spatially—are marked by different privacy norms. I should expect whatever I say on Speakers' Corner to be retold to anyone. I expect no-one to enter my house or observe me when the curtains are drawn without my permission. Pubs and pavements are intermediary spaces. I reasonably expect someone not to follow me without good reason while there, but I have no right not to be recognised or greeted.

5. Security is not binary but comes in degrees. Security is a function of the severity of possible harm and the likelihood of harm. In protecting society, the state fulfils its 'first' duty by mitigating risk to an acceptable level. The level of acceptable risk is a collective, political decision. It mitigates risk by taking measures to ameliorate the severity of possible harm; to reduce its likelihood through deterrence, detection and prevention; and to reduce uncertainty regarding both inputs.

Snowden revelations

6. Two points are noteworthy regarding the data collection practices revealed by Snowdon to have been employed by the NSA and GCHQ. The first is common knowledge. The second is of equal significance but less widely noted.

7. *Bulk collection of metadata*. The bulk collection of metadata makes possible an unprecedented depth of 'inferential disclosure' about a person's life.[1] Although inferential disclosure has in principle been possible before, the quantitative increase of volume and detail of information yielded by metadata constitutes a qualitative change. Metadata can often reveal content alone, including highly sensitive content (think of an extended telephone call to a domestic abuse or debt hotline). When aggregated over time it reveals enduring interests (e.g. repeated visits to a website). When aggregated over people it reveals a person's networks, the nature of those relationships, the shape of organisations, and even predicts a person's personality traits. The NSA and GCHQ have actively pursued new sources of metadata, thereby increasing the number of information channels available regarding a particular target. Metadata is of particular intelligence value here at least in part because it is easily stored and searched, thereby decreasing the time required for assessment.

8. *Culture*. One of the slides released as part of the Snowdon files contains a revealing scribble. Depicting the 'Public Cloud' and 'Google Cloud' and a single point of vulnerability between them, the NSA employee writes 'SSL added and removed here!' and alongside it a smiley face, '☺'. (See Naughton 2013.) The writer is not merely pointing out an efficient way to intercept Internet traffic. He or she is expressing delight at a cool hack.

This indicates a wider problem. The issue is not that people in the NSA and GCHQ enjoy doing their work; that is entirely welcome. The issue is that hacker culture and the technical skill set required for this kind of work come together. In the normal case, you get the skill set only by immersing yourself in the tech world and thereby being inducted into the culture. One challenge is that the culture's norms are orthogonal to civil society's norms. It takes some nimble thinking to make them align, and this thinking is inessential to active membership of the tech world. Another challenge it poses is that effective oversight requires commitment to upholding the norms of civil society *and* technological literacy.

Significance for security

9. Bulk metadata is significant for the pursuit of security in two important respects. For one, it allows intelligence agencies to confirm or deny reasonable suspicions of criminal or terrorist activity. When a person is the object of reasonable suspicion, metadata allows a detailed pattern of life to be constructed. This includes garnering evidence about interests and thereby possible intentions, as well as linking them with known or unknown associates, as a basis for threat assessment. In this respect, metadata is a new resource for a task that has long been performed by the police and intelligence agencies. In fulfilling this function, the metadata is valuable insofar as it relates to specific suspected individuals. The value of its 'bulkness' consists in the increased likelihood of coverage; that, for any suspected individual, the state is able to access metadata relevant to that target. In principle, data that does not relate to a suspected individual need never be examined by a person, even though it is held and may be computed during searches. Call this use of bulk data, *targeted threat investigation*.

10. Bulk metadata is also important prospectively. Patterns in collected metadata enable the prediction of future behaviour, and in this case, of future targets. The power of predictive analytics is well illustrated in the commercial sphere by the ability of Target, the American retail chain, to predict the due dates of its pregnant

[1] We ignore the US/UK distinction between *metadata* and *communications data*. Given that communications data is defined more restrictively than metadata, the degree of inferential disclosure possible is importantly restricted in the UK when compared to the US. But it is nonetheless extensive.

shoppers based solely on changes to shopping habits (Duhigg 2012). Once metadata has been aggregated from sufficiently many targets to have been verified actually to pose security threats, these profiles can be used to identify individuals hitherto unknown to the security services who may merit investigation. It is not possible for data used for this purpose to relate only to individuals who are the objects of reasonable suspicion. 'False positives' are inevitable, where a person is predicted to pose a threat but does not. In these cases a person rather than a machine must distinguish between true and false positives, preparatory to targeted investigation. Call this use of bulk data, *predictive threat investigation*.

Policy recommendation 1—Forego predictive analytics

11. The UK Government should forego the opportunity to develop and maintain predictive threat investigation capabilities. Whether the UK should do so is a fundamental political question, regarding the degree of risk we are prepared to bear. The paragraphs below are offered a contribution to that debate.

12. In non-totalitarian states, the established moral norm is that citizens' lives should be free from Government surveillance and investigation. The only exception is when there is reasonable suspicion of criminality or terrorism. The Snowden revelations show this norm to have been systematically breached. The burden of proof is on those who would revise this established standard, and it requires a good argument to justify it. We contend that are no such arguments. The two most commonly proposed—based on changing notions of privacy and increased threat—are fallacious.

13. *Privacy argument*. Arguments for why the UK should possess predictive threat investigation capabilities commonly focus on the changing nature of privacy. It is claimed that there is a generational shift, with the first 'i-Generation' now used both to having made available unprecedented amounts of personal information online as well as managing their online profiles more carefully. This line of argument holds that privacy is an illusion and we need to learn to live with the world as it is. If the commercial sphere is using predictive analytics, why would it be anything but irresponsible for the state not to use such public information for security purposes? (See Chesterman 2011.)

14. This is a bad argument. There are two problems. For one, the great majority of personal information sent via the Internet is disclosed with individuals' consent, on websites and through applications they have chosen to use. People agree to give their information to other parties they deal with, and frequently are invited to grant rights for data to be transferred. But consent is restricted to those parties, *not* to anyone else. It is a breach of confidentiality to procure such information, and requires justification for it to occur. Crucially, the moral norms which govern the marketplace are different to those which govern states' actions. Consent is given in the former but not the latter. (It is an important question whether a user's indication that they have read the terms and conditions of the End User Licence Agreement actually meets the conditions for informed consent. If not, there is an argument for consumer protection from exploitation by *de facto* monopolies. But that is a separate issue.)

15. For another, there is nothing inevitable about the 'de-privatisation' of life as a result of online interaction. Technological determinism is fallacious. We are at an historical moment where we are able collectively to influence the social norms which govern this new domain of interaction. In particular, it is up for

determination whether online interaction (or more realistically, what kinds of online interaction) should be considered public, private, or something in between, according to how we treat others there.

Parliament has a special role in influencing societal norms, given its role as the nation's debating chamber and legislator. The reasonable person regards themselves as bound morally to obey the law (Hart 1994). The laws Parliament enacts also express collective approval or disapproval of kinds of actions (Feinberg 1965; Sunstein 1996). Both constitute reasons for acting in accordance with legal norms, and regarding oneself and others as obliged to act in accordance. Once sufficiently many people follow a law, a new convention is established (Marmor 2009).

Because social norms can be influenced in this way, it is important that Parliament act on its responsibility to facilitate the emergence of pro-social, positive norms. There are two potential norms currently vying. One is that one's online actions are private, unless one consents to the contrary or strong reasons override. Another is that one's online actions are public, open to anyone's scrutiny. We contend that the former norm is preferable to the latter. This is because the kind of fundamental freedoms which mark a healthy democracy—such as genuine freedom of association and freedom of reading—require it. It is an abdication of responsibility to throw our hands up and say "nothing's private anymore anyway". Insofar as the UK Government decides whether or not to surveil the Internet at will, it helps establish the convention which will prevail.

16. An historical analogy illustrates the point. The centralised mail service established in London was first made available to the public in 1635 by Charles I. At issue then was the question: should the state read the letters to which it now had access? During the Civil War, John Thurloe as Spymaster-General established the Roundheads in the practice of opening and reading the letters while they were being sorted at night. Samuel Morland, part of this department, gave the justification.

'A skilful Prince ought to make a Watch Tower of his Gen[eral] Post Office ... & there ... place such carefull Centinels as that by their care and diligence he may have a constant view of all that passes. ... By the frequent inspection of letters ... a king soon knows the temper of all his principal and active subjects.' (Marshall 2003: 81, 84)

The practice had its effect. Edward Arden, secretary to the Bishop of Durham and uninvolved personally in the lethal politics of the day, feared to write much in one 'for letters are open'd and nothing is certain' (2003: 84). By the 1690s William III declined to continue the practice. Although letters were (and presumably still are) intercepted, such surveillance is not standard and requires specific justification for each case. The Royal Mail was, for its time, a new way for people to interact. There were two principal privacy conventions which could have been settled on. In one, mail was open to the state; in the other, it was private. Both are possible, and once established, we would all have learned to live with whichever convention had been adopted. But we regard it as a good thing that the former convention prevailed. Note that Morland's justification for reading the post remains apposite for those who would surveil the Internet. Arden's circumspection remains the rational response when it is surveilled. It is better, for individuals and a healthy polity, that that result be avoided.

17. This is not a simple-minded reiteration of the claim that 'Gentlemen don't read each other's mail', with which Harry Stimson, the then US Secretary of State, closed down their Cipher Bureau in 1929. Stimson's claim, while true, does not count against communications interception per se. Gentlemen may well not read each other's mail, but states certainly read other states' mail if they can get away with it. The present point is that they should not read their own citizens' mail. (Views differ as to whether they should read the mail of other countries' citizens; we ignore this issue here.)

18. *Increased threat argument*. There is another common form of argument which justifies more intrusive data collection and surveillance practices. The nature of the terrorist threat has changed, it is claimed, because biological and chemical weapons and cyberattacks are now achievable for groups with limited financial and organisational means. Attacks now are potentially catastrophic whereas previously the lives lost and value of property damaged was modest. So detection is increasingly important to mitigate the increased risk, towards maintaining an acceptable level of security. Liberties may need to be sacrificed to achieve this. (Persson and Savulescu 2012 make this claim, for instance.)

19. We are unpersuaded. For those without appropriate access, it is unknowable what kinds of plots have been prevented and what the possible loss of life would have been otherwise. Nonetheless, the loss of life in England and Wales due to terrorist attack since 2000 has been roughly equivalent to that from bee and wasp stings (Anderson 2012: 27). In the USA, over the past four decades, it is about the same as that from allergic reactions to peanuts (Bobbit 2008: 7). For much of this time, it has been possible to make homemade biological and chemical weapons without excessive difficulty, yet loss of life has been minimal. Whatever the explanation—whether effective intelligence work and damage limitation preparation, or absence of serious intention by competent groups—mass loss of life has been limited to 9/11. The burden is on those who would maintain the capability for predictive threat investigation to show its necessity.

Policy recommendation 2—Non-state data storage

20. The UK should retain and develop targeted threat investigation capabilities, but in ways that minimise pernicious effects on privacy. In particular, the Government should not hold metadata. This has radical implications. GCHQ should cease its bulk collection of metadata.

21. It is important for security purposes that the UK retains and develops the ability for targeted threat investigation. This is no change to prior practice. However, how that capability is implemented may respect existing privacy boundaries, or it may breach them. Data acquisition and storage by government breaches them. Data acquisition and storage by private companies which customers' consensually disclose to them respects it. We commend President Obama's recent instruction to the NSA to identify ways to ensure that metadata storage occurs with those who handle the data in the first place—the phone and Internet companies who deliver services to customers. Parallel proposals are supported for the UK.

22. The 'bulkness' of the communications data available for targeted threat investigation is not significantly impacted by this proposal. All the data that is currently being collected by corporations on the basis of customers' consent will remain accessible. It is just that it must be accessed from those corporations under conditions laid down by statute by the intelligence agencies.

Policy recommendation 3—Re-categorisation

23. Access to communications data should be re-categorised as directed surveillance. The current legal framework deals with access to communications data in Pt 1 Ch 2 of RIPA (2000), and allows considerable

latitude to officials' discretion for access. But the degree of revelation of personal information is considerably greater than there recognised. The GPS trail yielded by a mobile phone is as detailed as that provided by tailing the target, for instance. So access to communications data should be granted under the same conditions as permission given to tail someone, namely the conditions required for directed surveillance as specified in Pt 2 of RIPA (2000).

Policy recommendation 4—Competent oversight

24. Arrangements for GCHQ oversight should include independent individuals who are regarded as trustworthy by the wider public, and possess expert knowledge of the technologies employed by the security agencies.

25. Trust is an inescapable requirement for oversight of the intelligence services. Because their work is necessarily secret, transparency—the usual solution for ensuring accountable government—is inapplicable. So the public is unavoidably reliant on the word of those charged with exercising oversight that the intelligence agencies' conduct is within the law. For the public's trust to be rational, they must be assured that those overseers are trustworthy; that is, competent and motivated. In this case, this requires both independence, such that they are unafraid to expose wrongdoing, and technological expertise. The suspicion of regulatory capture is debilitating.

26. Since 2000, the three Interception of Communications Commissioners—responsible for overseeing the implementation of the Regulation of Investigatory Powers Act 2000 (RIPA)—have had legal expertise. They should be assisted by someone with technological expertise, cleared to the appropriate level and given wide-ranging access within GCHQ such that they can confirm that technical capabilities do not exceed that permitted by Parliament.

References

David Anderson. 2012. *The Terrorism Acts in 2011*. London: Stationary Office
Philip Bobbit. 2008. *Terror and Consent*. New York: Allen Lane
Simon Chesterman. 2011. *One Nation Under Surveillance*. Oxford: OUP
Charles Duhigg. 2012. *The Power of Habit*. London: Heinemann
Joel Feinberg. 1965. 'The Expressive Function of Punishment'. *Monist* 49 (3): 397-423
Thomas Hobbes. 1651. *Leviathan*
Alan Marshall. 2003. *Intelligence and Espionage in the Reign of Charles II 1660-1685*. Cambridge: CUP
Andrei Marmor. 2009. *Social Conventions: From Language to Law*. Princeton University Press
John Naughton. 2013. 'Why NSA's war on terror is more than just a 'neat' hacking game'. At <http://www.theguardian.com/world/2013/nov/10/nsa-war-on-terror-neat-hacking-game>, accessed 4 Feb 14
Ingmar Persson and Julian Savulescu. 2012. *Unfit for the Future: The Need for Moral Enhancement*. Oxford: OUP
Adam Smith. 1776. *The Wealth of Nations*
Cass R. Sunstein. 1996. On the Expressive Function of Law. *University of Pennsylvania Law Review* 144: 2021–53